Use SAML

SANtricity 11.9

NetApp
December 16, 2024

Índice

Use SAML

Configurar SAML

Para configurar a autenticação para o Access Management, você pode usar os recursos de Security Assertion Markup Language (SAML) incorporados no storage array. Esta configuração estabelece uma conexão entre um Provedor de identidade e o Provedor de armazenamento.

Antes de começar

- Você deve estar conetado com um perfil de usuário que inclua permissões de administrador de segurança. Caso contrário, as funções de Gerenciamento de Acesso não aparecem.
- Você deve saber o endereço IP ou o nome de domínio do controlador na matriz de armazenamento.
- Um administrador de IDP configurou um sistema de IDP.
- Um administrador de IDP garantiu que o IDP suporta a capacidade de retornar um ID de nome na autenticação.
- Um administrador garantiu que o servidor IDP e o relógio do controlador são sincronizados (através de um servidor NTP ou ajustando as definições do relógio do controlador).
- Um arquivo de metadados IDP é baixado do sistema IDP e está disponível no sistema local usado para acessar o Unified Manager.

Sobre esta tarefa

Um Provedor de identidade (IDP) é um sistema externo usado para solicitar credenciais de um usuário e para determinar se esse usuário foi autenticado com êxito. O IDP pode ser configurado para fornecer autenticação multifator e usar qualquer banco de dados de usuários, como o ative Directory. Sua equipe de segurança é responsável por manter o IDP. Um provedor de serviços (SP) é um sistema que controla a autenticação e o acesso do usuário. Quando o Gerenciamento de Acesso é configurado com SAML, o storage array atua como o provedor de serviços para solicitar autenticação do provedor de identidade. Para estabelecer uma conexão entre o IDP e o storage array, você compartilha arquivos de metadados entre essas duas entidades. Em seguida, você mapeia as entidades de usuário IDP para as funções de storage array. E, finalmente, você testa os logins de conexão e SSO antes de ativar o SAML.

SAML e Serviços de diretório. Se você ativar o SAML quando os Serviços de diretório estiverem configurados como o método de autenticação, o SAML substituirá os Serviços de diretório no Unified Manager. Se você desabilitar o SAML mais tarde, a configuração dos Serviços de diretório retornará à configuração anterior.

Edição e desativação. Uma vez que o SAML está ativado, você *não pode* desabilitá-lo através da interface do usuário, nem pode editar as configurações de IDP. Se você precisar desativar ou editar a configuração SAML, entre em Contato com o suporte técnico para obter assistência.

Configurar a autenticação SAML é um procedimento de várias etapas.

Passo 1: Faça o upload do arquivo de metadados IDP

Para fornecer ao storage array informações de conexão IDP, você importa metadados IDP para o Unified Manager. O sistema de IDP precisa desses metadados para redirecionar as solicitações de autenticação para o URL correto e para validar as respostas recebidas.

Passos

1. Selecione **Definições › Gestão de Acesso**.
2. Selecione a guia **SAML**.

   A página exibe uma visão geral das etapas de configuração.

3. Clique no link **Import Identity Provider (IDP) file**.

   A caixa de diálogo Importar arquivo do provedor de identidade será aberta.

4. Clique em **Procurar** para selecionar e carregar o ficheiro de metadados IDP copiado para o sistema local.

   Depois de selecionar o ficheiro, é apresentado o ID da entidade IDP.

5. Clique em **Importar**.

Passo 2: Exportar arquivos do provedor de serviços

Para estabelecer uma relação de confiança entre o IDP e o storage array, você importa os metadados do provedor de serviços para o IDP. O IDP precisa desses metadados para estabelecer uma relação de confiança com o controlador e processar solicitações de autorização. O arquivo inclui informações como o nome de domínio do controlador ou endereço IP, para que o IDP possa se comunicar com os provedores de serviços.

Passos

1. Clique no link **Exportar arquivos do provedor de serviços**.

   A caixa de diálogo Exportar ficheiros do fornecedor de serviços abre-se.

2. Introduza o endereço IP do controlador ou o nome DNS no campo **Controller A** e, em seguida, clique em **Export** para guardar o ficheiro de metadados no sistema local.

   Depois de clicar em **Exportar**, os metadados do fornecedor de serviços são transferidos para o seu sistema local. Anote onde o arquivo é armazenado.

3. No sistema local, localize o arquivo de metadados do provedor de serviços formatado em XML que você exportou.
4. A partir do servidor IDP, importe o arquivo de metadados do provedor de serviços para estabelecer a relação de confiança. Você pode importar o arquivo diretamente ou inserir manualmente as informações do controlador a partir do arquivo.

Passo 3: Mapear funções

Para fornecer aos usuários autorização e acesso ao Unified Manager, é necessário mapear os atributos de usuário e associações a grupos de IDP para as funções predefinidas do storage array.

Antes de começar

- Um administrador de IDP configurou atributos de usuário e associação de grupo no sistema de IDP.
- O arquivo de metadados de IDP é importado para o Unified Manager.
- Um arquivo de metadados do provedor de serviços para o controlador é importado para o sistema IDP para a relação de confiança.

Passos

1. Clique no link para **Mapping Unified Manager** Roles.

   A caixa de diálogo Mapeamento de função é aberta.

2. Atribua atributos de usuário e grupos IDP às funções predefinidas. Um grupo pode ter várias funções atribuídas.

   Detalhes do campo

Definição	Descrição
Mapeamentos	Atributo do utilizador
Especifique o atributo (por exemplo, "membro de") para o grupo SAML a ser mapeado.	Valor do atributo
Especifique o valor do atributo para o grupo a ser mapeado. Expressões regulares são suportadas. Esses carateres especiais de expressão regular devem ser escapados com uma barra invertida (\) se eles não forem parte de um padrão de expressão regular	Funções

   A função Monitor é necessária para todos os usuários, incluindo o administrador. O Unified Manager não funcionará corretamente para nenhum usuário sem a função Monitor presente.

3. Se desejar, clique em **Adicionar outro mapeamento** para inserir mais mapeamentos de grupo para função.

   Mapeamentos de função podem ser modificados depois que o SAML estiver habilitado.

4. Quando terminar com os mapeamentos, clique em **Salvar**.

Passo 4: Teste o login SSO

Para garantir que o sistema IDP e o storage array possam se comunicar, você pode testar opcionalmente um login SSO. Este teste também é realizado durante a etapa final para ativar o SAML.

Antes de começar

- O arquivo de metadados de IDP é importado para o Unified Manager.

- Um arquivo de metadados do provedor de serviços para o controlador é importado para o sistema IDP para a relação de confiança.

Passos

1. Selecione o link **Test SSO Login**.

   Abre-se uma caixa de diálogo para introduzir credenciais SSO.

2. Insira credenciais de login para um usuário com permissões de Administrador de Segurança e permissões de Monitor.

   Abre-se uma caixa de diálogo enquanto o sistema testa o início de sessão.

3. Procure uma mensagem Teste bem-sucedida. Se o teste for concluído com êxito, vá para a próxima etapa para ativar o SAML.

   Se o teste não for concluído com êxito, é apresentada uma mensagem de erro com mais informações. Certifique-se de que:

   - O usuário pertence a um grupo com permissões para Administrador de Segurança e Monitor.
   - Os metadados carregados para o servidor IDP estão corretos.
   - O endereço do controlador nos arquivos de metadados do SP está correto.

Passo 5: Ative o SAML

Sua etapa final é concluir a configuração SAML para autenticação de usuário. Durante esse processo, o sistema também solicita que você teste um login SSO. O processo de teste SSO Login é descrito na etapa anterior.

Antes de começar

- O arquivo de metadados de IDP é importado para o Unified Manager.
- Um arquivo de metadados do provedor de serviços para o controlador é importado para o sistema IDP para a relação de confiança.
- Pelo menos um mapeamento de função Monitor e um Admin de segurança está configurado.

Edição e desativação. Uma vez que o SAML está ativado, você *não pode* desabilitá-lo através da interface do usuário, nem pode editar as configurações de IDP. Se você precisar desativar ou editar a configuração SAML, entre em Contato com o suporte técnico para obter assistência.

Passos

1. Na guia **SAML**, selecione o link **Ativar SAML**.

   A caixa de diálogo confirmar ativação SAML é aberta.

2. Digite `enable`e clique em **Ativar**.
3. Insira as credenciais do usuário para um teste de login SSO.

Resultados

Depois que o sistema ativa o SAML, ele termina todas as sessões ativas e começa a autenticar usuários por meio do SAML.

Alterar mapeamentos de função SAML

Se você configurou o SAML para Gerenciamento de Acesso anteriormente, poderá alterar os mapeamentos de função entre os grupos de IDP e as funções predefinidas do storage array.

Antes de começar

- Você deve estar conetado com um perfil de usuário que inclua permissões de administrador de segurança. Caso contrário, as funções de Gerenciamento de Acesso não aparecem.
- Um administrador de IDP configurou atributos de usuário e associação de grupo no sistema de IDP.
- O SAML está configurado e ativado.

Passos

1. Selecione **Definições › Gestão de Acesso**.
2. Selecione a guia **SAML**.
3. Selecione **Mapeamento de função**.

   A caixa de diálogo Mapeamento de função é aberta.

4. Atribua atributos de usuário e grupos IDP às funções predefinidas. Um grupo pode ter várias funções atribuídas.

   Tenha cuidado para não remover suas permissões enquanto o SAML estiver ativado ou você perderá o acesso ao Unified Manager.

   Detalhes do campo

Definição	Descrição
Mapeamentos	Atributo do utilizador
Especifique o atributo (por exemplo, "membro de") para o grupo SAML a ser mapeado.	Valor do atributo
Especifique o valor do atributo para o grupo a ser mapeado.	Funções

   A função Monitor é necessária para todos os usuários, incluindo o administrador. O Unified Manager não funcionará corretamente para nenhum usuário sem a função Monitor presente.

5. Opcionalmente, clique em **Adicionar outro mapeamento** para inserir mais mapeamentos de grupo para função.
6. Clique em **Salvar**.

Resultados

Depois de concluir esta tarefa, todas as sessões ativas do utilizador são encerradas. Apenas a sessão de utilizador atual é mantida.

Exporte arquivos do provedor de serviços SAML

Se necessário, você pode exportar metadados do provedor de serviços para o storage array e reimportar o arquivo para o sistema de provedor de identidade (IDP).

Antes de começar

- Você deve estar conetado com um perfil de usuário que inclua permissões de administrador de segurança. Caso contrário, as funções de Gerenciamento de Acesso não aparecem.
- O SAML está configurado e ativado.

Sobre esta tarefa

Nesta tarefa, você exporta metadados do controlador. O IDP precisa desses metadados para estabelecer uma relação de confiança com o controlador e processar solicitações de autenticação. O arquivo inclui informações como o nome de domínio do controlador ou endereço IP que o IDP pode usar para enviar solicitações.

Passos

1. Selecione **Definições › Gestão de Acesso**.
2. Selecione a guia **SAML**.
3. Selecione **Exportar**.

   A caixa de diálogo Exportar ficheiros do fornecedor de serviços abre-se.

4. Clique em **Exportar** para salvar o arquivo de metadados no sistema local.

   O campo de nome de domínio é somente leitura.

   Anote onde o arquivo é armazenado.

5. No sistema local, localize o arquivo de metadados do provedor de serviços formatado em XML que você exportou.
6. No servidor IDP, importe o arquivo de metadados do provedor de serviços. Você pode importar o arquivo diretamente ou inserir manualmente as informações do controlador.
7. Clique em **Fechar**.

Informações sobre direitos autorais

Informações sobre marcas comerciais